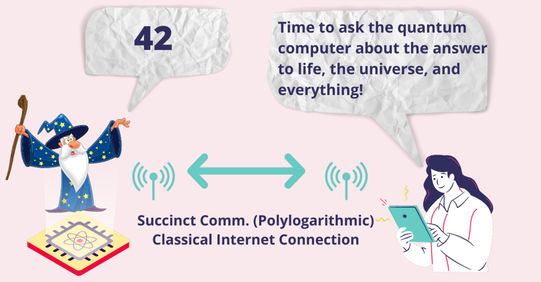
Interactive Oracle Arguments in the QROM and Applications to Succinct Verification of Quantum Computation

Islam Faisal

BUCS Boston University

Motivating Question

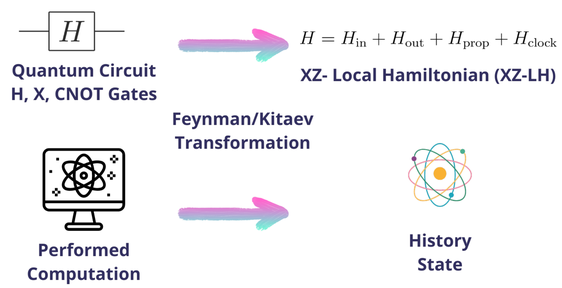


Can Merlin convince Alice of his answer?

Model and Assumptions

- The Quantum Random Oracle Model (QROM) [BODF+10, Zha18, DFMS21] with $\mathbf{RO} : \mathcal{X} \to \{0,1\}^\lambda$
- Non-succinct setup phase independent of the instance (task)
- Quantum Hardness of the Learning With Errors (LWE) problem
- XZ Quantum PCP Conjecture: XZ-LH problem is hard with $\tilde{O}(1)$ promise gap (Open Problem)

Step 1: Circuit-to-Hamiltonian



Step 2 [Mah18, ACGH20]: Convert the XZ-LH Proof System of [MNS16, MF16] into a Classical Argument

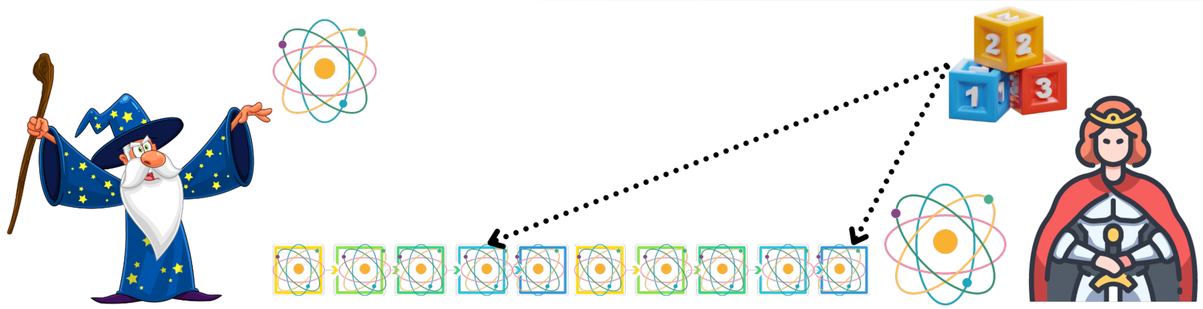
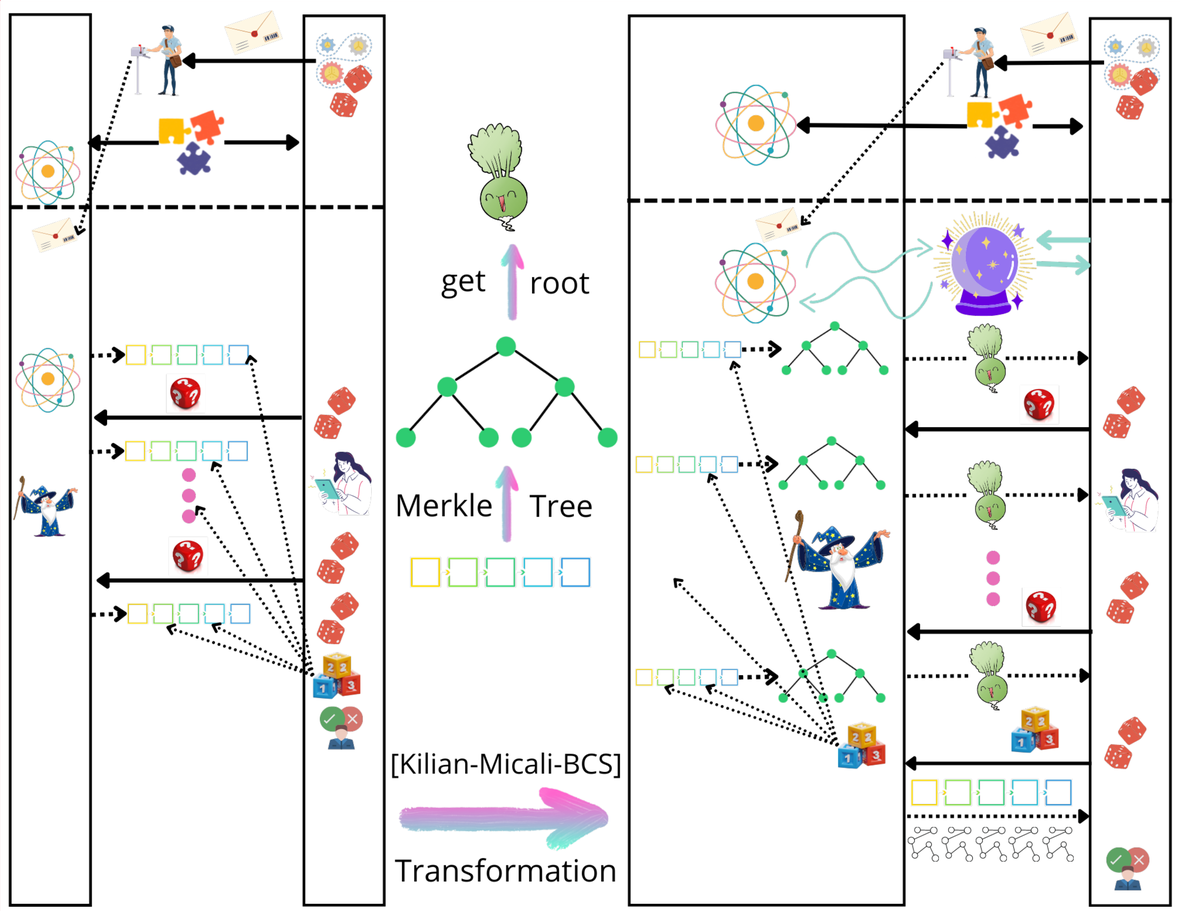


Illustration of the XZ-Quantum PCP Conjecture.
Step 2 when applied to XZ-LH proof system (a.k.a quantum PCP) with $\tilde{O}(1)$ query complexity yields an IOArg with succinct query complexity.

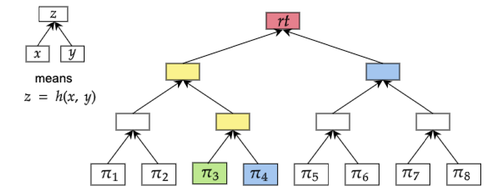
Step 3: Succinct Argument from Interactive Oracle Argument (IOArg)



Interactive Oracle Arguments (IOArgs) extend interactive oracle proofs (IOPs) [BSCS16].

Verifiable Measurement [Mah18]

Merkle Trees



A *Merkle tree* example of depth $d = 3$ to commit to $2^3 = 8$ *leaves* with the *root* rt.

Acknowledgements

Thanks to Mark Bun and Nicholas Spooner for their mentorship and help with refining and revising this project. I.F. is partially supported by NSF grants CCF-1947889 and CNS-1414119. Full acknowledgements list is in preprint.

Preprint

`https://eprint.iacr.org/2023/421`

References

[ACGH20] Gorjan Alagic, Andrew M. Childs, Alex B. Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation, 2020.

[BODF+10] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world, 2010.

[BSCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive oracle proofs, 2016.

[DFMS21] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model, 2021.

[Mah18] Urmila Mahadev. Classical Verification of Quantum Computations, 2018.

[MF16] Tomoyuki Morimae and Joseph F Fitzsimons. Post hoc verification with a single prover, 2016.

[MNS16] Tomoyuki Morimae, Daniel Nagaj, and Norbert Schuch. Quantum proofs can be verified using only single-qubit measurements, Feb 2016.

[Zha18] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability,